PAT-NO: JP409045008A

DOCUMENT-IDENTIFIER: JP 09045008 A

TITLE: DATA TRANSMITTING METHOD, DATA RECORDING APPARATUS, DATA RECORDING MEDIUM AND DATA REPRODUCING APPARATUS

PUBN-DATE: February 14, 1997

INVENTOR-INFORMATION:

NAME	COUNTRY
SAKO, YOICHIRO	
OSAWA, YOSHITOMO	
KURIHARA, AKIRA	
KAWASHIMA, ISAO	

ASSIGNEE-INFORMATION:

NAME	COUNTRY
SONY CORP	N/A

APPL-NO: JP07195191

APPL-DATE: July 31, 1995

INT-CL (IPC): G11B020/12 , G06F012/14 , G06F012/16 , G09C001/00 , H03M013/00 , H04L001/00 , H04L009/18

ABSTRACT:

PROBLEM TO BE SOLVED: To encrypt data in a simple constitution and access at high speed.

SOLUTION: In an error-correcting code format, a sector 73 is constituted of a head part 71 and a user data part 72. An error correction C1 direction is set in a R/W direction and a C1 parity 74 is generated and added. On the other hand, an error correction C2 direction is set in a direction oblique to the C1 direction and a C2 parity 75 is generated and added. Data excluding at least the head part 71, e.g., a part 76 in the same row as the head pat 71 among the

data handled in an **error-correcting code** process are converted in [illegible] with an **encryption** flag data.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－45008

(43)公開日　平成９年(1997)２月14日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ１１Ｂ	20/12	１０２	9295－5D	Ｇ１１Ｂ	20/12	１０２
Ｇ０６Ｆ	12/14	３２０		Ｇ０６Ｆ	12/14	３２０Ｂ
	12/16	３２０	7623－5B		12/16	３２０Ａ
Ｇ０９Ｃ	1/00	６６０	7259－5J	Ｇ０９Ｃ	1/00	６６０Ｄ
Ｈ０３Ｍ	13/00			Ｈ０３Ｍ	13/00	

審査請求　未請求　請求項の数７　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願平7－195191

(22)出願日　平成７年(1995)７月31日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　栗原　章
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　弁理士　小池　晃　（外２名）

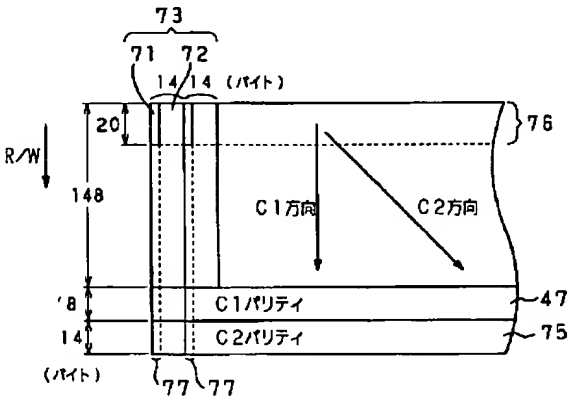
最終頁に続く

(54)【発明の名称】　データ伝送方法、データ記録装置、データ記録媒体及びデータ再生装置

(57)【要約】

【課題】　簡単な構成で暗号化を施すと共に、高速アクセスを可能とする。

【解決手段】　誤り訂正符号フォーマットにおいて、ヘッダ部７１とユーザデータ部７２とでセクタ７３が構成されており、Ｒ／Ｗ方向に誤り訂正のＣ１方向がとられてＣ１パリティ７４が生成付加され、これに対して斜めの方向に誤り訂正のＣ２方向がとられてＣ２パリティ７５が生成付加される。この誤り訂正符号化処理の際に取り扱われるデータの内の少なくともヘッダ部７１を除いたデータ、例えばヘッダ部７１と同一行の部分７６を除いたデータに対して、暗号化の鍵情報に応じたデータ変換を施す。



1

【特許請求の範囲】
【請求項1】　データの伝送単位がヘッダ部とユーザデータ部とを有して成る入力ディジタルデータに誤り訂正符号化処理を施して伝送するデータ伝送方法において、上記誤り訂正符号化処理の際に取り扱われるデータの内の少なくとも上記ヘッダ部を除いたデータに対して、暗号化の鍵情報に応じてデータ変換を施すことを特徴とするデータ伝送方法。
【請求項2】　上記データ変換は、データと暗号化の鍵情報との論理演算により行われることを特徴とする請求項1記載のデータ伝送方法。
【請求項3】　上記暗号化の鍵情報は、少なくとも一部に識別情報を含むことを特徴とする請求項1記載のデータ伝送方法。
【請求項4】　上記上記データ変換が行われるデータは、上記誤り訂正符号のマトリクスにおける上記ヘッダ部と同一行あるいは同一列のデータを除いたデータであることを特徴とする請求項1記載のデータ伝送方法。
【請求項5】　データの記録単位がヘッダ部とユーザデータ部とを有して成る入力ディジタルデータに誤り訂正符号化処理を施して記録媒体に記録するデータ記録装置において、
暗号化の鍵情報の入力手段と、
この入力手段からの鍵情報に応じて、上記誤り訂正符号化処理の際に取り扱われるデータの内の少なくとも上記ヘッダ部を除くデータに対してデータ変換を施す手段とを有することを特徴とするデータ記録装置。
【請求項6】　データの記録単位がヘッダ部とユーザデータ部とを有して成る入力ディジタルデータに誤り訂正符号化処理を施す際に取り扱われるデータの内の少なくとも上記ヘッダ部を除くデータに対して、暗号化の鍵情報に応じてデータ変換が施されて得られた信号が記録されて成ることを特徴とするデータ記録媒体。
【請求項7】　データの記録単位がヘッダ部とユーザデータ部とを有して成る入力ディジタルデータに対して誤り訂正符号化処理が施されて記録媒体に記録された信号を再生するデータ再生装置において、
上記誤り訂正符号化処理の際に取り扱われるデータの内の少なくとも上記ヘッダ部を除くデータに対して施されるデータ変換を示す暗号化の鍵情報を入力する鍵情報入力手段と、
上記誤り訂正符号化処理に対応する誤り訂正復号化処理を行うと共に、上記鍵情報入力手段からの暗号化の鍵情報に応じたデータに上記データ変換に対する復号化のためのデータ変換を施す誤り訂正復号化手段とを有することを特徴とするデータ再生装置。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、コピー防止や不正使用の阻止、あるいは課金システムに適用可能なデータ伝送方法、データ記録装置、データ記録媒体、及びデータ再生装置に関する。

2

【0002】
【従来の技術】近年において、光ディスク等のディジタル記録媒体の大容量化と普及により、コピー防止や不正使用の阻止が重要とされてきている。すなわち、ディジタルオーディオデータやディジタルビデオデータの場合には、コピーあるいはダビングにより劣化のない複製物を容易に生成でき、また、コンピュータデータの場合には、元のデータと同一のデータが容易にコピーできるため、既に不法コピーによる弊害が生じてきているのが実情である。
【0003】ディジタルオーディオデータやディジタルビデオデータの不法コピー等を回避するためには、例えばいわゆるＳＣＭＳ（シリアルコピー管理システム）やＣＧＭＳ（コピー世代管理システム）の規格が知られているが、これは記録データの特定部分にコピー禁止フラグを立てるようなものであるため、いわゆるダンプコピー等の方法によりデータを抜き出される問題がある。
【0004】また、コンピュータデータ等のファイル内容自体を暗号化し、それを正規の登録された使用者にのみ使用許諾することが行われている。これは、情報流通の形態として、情報が暗号化されて記録されたディジタル記録媒体を配布したり、暗号化されたディジタル信号を有線、無線の伝送路を介して容易に入手可能にしておき、使用者が必要とした内容について料金を払って鍵情報を入手し、暗号を解いて利用可能とするようなシステムに結び付くものであるが、簡単で有用な暗号化の手法の確立が望まれている。
【0005】
【発明が解決しようとする課題】ところで、データの暗号化の際に、データ記録単位あるいは伝送単位となるセクタのヘッダ部分の同期（シンク）やアドレスのデータが暗号化されていると、暗号を解かないと同期やアドレスの情報が得られないため、高速アクセスの障害となることがある。
【0006】本発明は、上述したような実情に鑑みてなされたものであり、簡単な構成で暗号化が行え、暗号の難易度あるいは深度の制御も容易に行え、また、高速アクセス性の劣化等の弊害も生じないようなデータ伝送方法、データ記録装置、データ記録媒体、及びデータ再生装置の提供を目的とする。
【0007】
【課題を解決するための手段】上記の課題を解決するために、本発明は、誤り訂正符号化処理の際に取り扱われるデータの内の少なくともヘッダ部を除いたデータに対して、暗号化の鍵情報に応じたデータ変換を施すことを特徴としている。このデータ変換としては、データと上記鍵情報との論理演算を挙げることができる。上記鍵情報の一部に媒体や装置等の識別情報を含ませてもよい。

なお、上記ヘッダ部とは、データ伝送単位あるいは記録単位となる例えばセクタの先頭位置に配置されている部分で、セクタシンクやセクタアドレス等を含むものである。

【０００８】また、本発明に係るデータ記録媒体は、誤り訂正符号化処理を施す際に取り扱われるデータの内の少なくともヘッダ部を除いたデータに対して、暗号化の鍵情報に応じたデータ変換が施されて得られた信号が記録されて成ることを特徴としている。

【０００９】さらに、本発明に係るデータ再生方法は、誤り訂正符号化処理の際に取り扱われるデータの内の少なくともヘッダ部を除いたデータに対して、暗号化の鍵情報に応じたデータ変換が施されており、対応する誤り訂正復号化処理の際に取り扱われるデータの内の上記暗号化の鍵情報に応じたデータに上記データ変換に対する復号化のためのデータ変換を施すことを特徴としている。

【００１０】誤り訂正符号化処理の際に取り扱われるデータのヘッダ部を除くデータに対して、暗号化の鍵情報に応じたデータ変換を施すことにより、ヘッダ部については暗号化の復号化処理を介さずに再生できる。再生時に鍵情報に応じた暗号の復号化のためのデータ変換を施さないと、訂正不能誤りの個数が増加する。データ変換を施すデータの個数を変化させることにより、所望の暗号化の難易度を実現できる。

【００１１】

【発明の実施の形態】以下、本発明の好ましい実施の形態について図面を参照しながら説明する。

【００１２】図１は、本発明の実施の形態が適用されるデータ記録装置を概略的に示すブロック図である。この図１において、入力端子１１には、例えばアナログのオーディオ信号やビデオ信号をディジタル変換して得られたデータやコンピュータデータ等のディジタルデータが供給されている。この入力ディジタルデータは、インターフェース回路１２を介して、セクタ化回路１３に送られ、所定データ量単位、例えば２０４８バイト単位でセクタ化される。セクタ化されたデータは、スクランブル処理回路１４に送られてスクランブル処理が施される。この場合のスクランブル処理は、同一バイトパターンが連続して表れないように、すなわち同一パターンが除去されるように、入力データをランダム化して、信号を適切に読み書きできるようにすることを主旨としたランダム化処理のことである。スクランブル処理あるいはランダム化処理されたデータは、ヘッダ付加回路１５に送られて、各セクタの先頭に配置されるヘッダデータが付加された後、誤り訂正符号化回路１６に送られる。誤り訂正符号化回路１６では、データ遅延及びパリティ計算を行ってパリティを付加する。次の変調回路１７では、所定の変調方式に従って、例えば８ビットデータを１６チャンネルビットの変調データに変換し、同期付加回路１８に送る。同期付加回路１８では、上記所定の変調方式の変調規則を破る、いわゆるアウトオブルールのパターンの同期信号を所定のデータ量単位で付加し、駆動回路すなわちドライバ１９を介して記録ヘッド２０に送っている。記録ヘッド２０は、例えば光学的あるいは磁気光学的な記録を行うものであり、ディスク状の記録媒体２１に上記変調された記録信号の記録を行う。このディスク状記録媒体２１は、スピンドルモータ２２により回転駆動される。

【００１３】なお、上記スクランブル処理回路１４は、ヘッダ付加回路１５の後段に挿入して、ヘッダ付加されたディジタルデータに対してスクランブル処理を施して誤り訂正符号化回路１６に送るようにしてもよい。

【００１４】ここで、上記誤り訂正符号化回路１６は、誤り訂正符号化処理の際に取り扱われるデータの内の上記ヘッダ部を除いたデータに対して、暗号化の鍵情報に応じたデータ変換を施すような構成を有している。

【００１５】この誤り訂正符号化回路１６の構成の具体例を図２、図３に示す。これらの図２、図３において、入力端子５１には、上記図１のヘッダ付加回路１５からのデータが第１の符号化器であるＣ１エンコーダ５２に供給されている。この具体例においては、誤り訂正符号化の１フレームは１４８バイトあるいは１４８シンボルのデータから成るものとしており、入力端子５１からのディジタルデータが１４８バイト毎にまとめられて、第１の符号化器であるＣ１エンコーダ５２に供給される。Ｃ１エンコーダ５２では８バイトのＰパリティが付加され、インターリーブのための遅延回路５３を介して第２の符号化器であるＣ２エンコーダ５４に送られる。Ｃ２エンコーダ５４では１４バイトのＱパリティが付加され、このＱパリティは遅延回路５５を介してＣ１エンコーダ５２に帰還されている。このＣ１エンコーダ５２からのＰ、Ｑパリティを含む１７０バイトが取り出されて、遅延回路５６を介し、図３のインバータ部５７ａを有する再配列回路５７を介して出力され、図１の変調回路１７に送られる。

【００１６】このような誤り訂正符号化回路において、内部で取り扱われるデータの内のヘッダ部を除いたデータに対して、暗号化の鍵情報に応じてデータ変換を施すような暗号化処理としては、例えば再配列回路５７内のインバータ部５７ａの各バイト毎に、暗号の鍵情報に応じてインバータを入れるか入れないかの選択を行わせるようにすることが挙げられる。すなわち、基準構成においては、２２バイトのＰ、Ｑパリティに対して再配列回路５７のインバータ部５７ａによる反転が行われて出力されるが、これらのインバータ部５７ａ内のインバータのいくつかを無くしたり、Ｃ１データ側にいくつかのインバータを入れて反転して出力させたりすることが挙げられる。

【００１７】このようなデータ変換を施す場合、基準構

成からの違いの程度によって誤り訂正不能確率が変化し、違いが少ないときには最終的な再生出力におけるエラー発生確率がやや高くなる程度であるのに対し、違いが多いときには全体的にエラー訂正が行われなくなって殆ど再生できなくなるような状態となる。すなわち、例えばC1エンコーダについて見ると、誤り訂正能力を示す指標であるいわゆるディスタンスが9であるため、最大4バイトまでのエラー検出訂正が行え、消失（イレージャ）ポインタがあれば最大8バイトまでの訂正が可能であることから、違いが5箇所以上あると、C1符号では常に訂正不可となる。違いが4箇所の場合は、他に1バイトでもエラーが生じると訂正不可という微妙な状態となる。違いが3、2、1箇所と減少するにつれて、誤り訂正できる確率が増えてゆく。これを利用すれば、オーディオやビデオのソフトを提供する場合等に、ある程度は再生できるが完璧ではなく時々乱れる、といった再生状態を積極的に作り出すことができ、該ソフトの概要だけを知らせる用途等に使用することができる。

【0018】この場合、予めインバータの変更を行う場所を例えば2箇所程度規定しておく方法と、変更箇所を鍵情報に応じてランダムに選び、最低個数を2箇所程度に制限する方法と、これらを複合する方法とが挙げられる。

【0019】さらに、インバータの挿入あるいは変更位置としては、図2の再配列回路57の位置に限定されず、例えばC1エンコーダ52の前段や後段等の他の位置やこれらの位置を組み合わせるようにしてもよい。複数の位置の場合に、異なる鍵を用いるようにしてもよい。また、上記データ変換としては、インバータを用いる以外に、ビット加算や種々の論理演算を用いるようにしたり、データを暗号化の鍵情報に応じて転置するようにしたり、データを暗号化の鍵情報に応じて置換するようにしてもよい。

【0020】次に、上記誤り訂正符号化回路で取り扱われるデータの内のヘッダ部について説明する。

【0021】図4はセクタフォーマットの具体例を示しており、1セクタは、2048バイトのユーザデータ領域41に対して、4バイトの同期領域42と、16バイトのヘッダ領域43と、4バイトの誤り検出符号（EDC）領域44とが付加されて構成されている。誤り検出符号領域44の誤り検出符号は、ユーザデータ領域41及びヘッダ領域43に対して生成される32ビットのCRC符号から成っている。

【0022】ヘッダ領域43内には、図4に示すように、いわゆる巡回符号であるCRC45、コピーの許可／不許可やコピー世代管理等のためのコピー情報46、多層ディスクのどの層かを示す層（レイヤ）47、アドレス48、予備49の各領域が設けられている。

【0023】ここで、本発明の実施の形態におけるヘッダ部は、同期すなわちセクタシンクとヘッダ情報とを含むものであり、上記図4の例では、4バイトの同期領域42と16バイトのヘッダ領域43との計20バイトのデータがヘッダ部のデータである。残りのユーザデータ領域41及び誤り検出符号（EDC）領域44がユーザデータ部となる。

【0024】このようなヘッダ部とユーザデータ部に対して、クロスインターリーブ型の誤り訂正符号化を施すときの誤り訂正フォーマットを図5に示す。

【0025】この図5の例は、上記図4のセクタフォーマットのデータを上記図2、図3の誤り訂正符号化回路にて誤り訂正符号化処理するときの様子を示し、20バイトのヘッダ部71と2052バイトのユーザデータ部72とで、2072バイトのセクタ73が構成されている。このセクタは、記録／再生方向であるR／W方向に148バイト、これと直交する方向に14バイトの2次元に配列され、R／W方向に誤り訂正のC1方向がとられて8バイトのC1パリティ74が生成付加され、これに対して斜めの方向に誤り訂正のC2方向がとられて14バイトのC2パリティ75が生成付加されている。この図5の誤り訂正フォーマットのR／W方向の先頭20バイトのヘッダ部71と同一行の部分76を除いた部分に対して、上記データ変換を行っている。なお、図5のヘッダ部71と同一列の部分77を除いた部分に対して、上記データ変換を行わせてもよく、これらを組み合わせるようにしてもよい。

【0026】ここで図6は、上記誤り訂正符号化回路16の他の具体例として、再配列回路57内のインバータ部57aの後段すなわち出力側の位置に、データ変換手段としての排他的論理和（ExOR）回路群61を挿入し、C1エンコーダ52の前段すなわち入力側の位置にも、データ変換手段としてのExOR回路群66を挿入した例を示している。

【0027】これらのデータ変換手段としてのExOR回路群61、66は、誤り訂正フォーマットの上記図5の部分76に相当する20バイト分を除くデータに対してデータ変換を行うものである。具体的に、ExOR回路群61は、C1エンコーダ52から遅延回路56、及び上記再配列回路57のインバータ部57aを介して取り出される170バイトのデータ、すなわち情報データ$C1_{170n+169}$～$C1_{170n+22}$及びパリティデータ$P1_{170n+21}$～$P1_{170n+14}$、$Q1_{170n+13}$～$Q1_{170n}$の内、先頭の20バイトのデータ$C1_{170n+169}$～$C1_{170n+150}$を除いた残り150バイトのデータ$C1_{170n+149}$～$Q1_{170n}$に対して排他的論理和（ExOR）回路を用いたデータ変換を行い、ExOR回路群66は、148バイトの入力データB_{148n}～$B_{148n+147}$の内、先頭の20バイトのデータB_{148n}～$B_{148n+19}$を除いた残り128バイトのデータ$B_{148n+20}$～$B_{148n+147}$に対して排他的論理和（ExOR）回路を用いたデータ変換を行う。これらのExOR回路群61、66に用いられるExOR回路は、1

バイトすなわち8ビットの入力データと1ビットの制御データで指示される所定の8ビットデータとの排他的論理和（ExOR）をそれぞれとるような8ビットExOR回路であり、このような8ビットExOR回路（所定の8ビットデータがオール1の場合はインバータ回路に相当する）が、ExOR回路群61では150個、ExOR回路群66では128個用いられている。

【0028】この図6においては、150ビットの鍵情報が端子62に供給され、いわゆるDラッチ回路63を介してExOR回路群61内の150個の各ExOR回路にそれぞれ供給されている。Dラッチ回路63は、イネーブル端子64に供給された1ビットの暗号化制御信号に応じて、端子62からの150ビットの鍵情報をそのままExOR回路群61に送るか、オールゼロ、すなわち150ビットの全てを“0”とするかが切換制御される。ExOR回路群61の150個の各ExOR回路の内、Dラッチ回路63から“0”が送られたExOR回路は、上記再配列回路57の内のインバータ部57aからのデータをそのまま出力し、Dラッチ回路63から“1”が送られたExOR回路は、上記再配列回路57のインバータ部57aからのデータを変換して出力する。オールゼロのときには、上記再配列回路57のインバータ部57aからのデータをそのまま出力することになる。また、ExOR回路群66については、128個のExOR回路を有し、鍵情報が128ビットであること以外は、上記ExOR回路群61の場合と同様であり、端子67に供給された128ビットの鍵情報がDラッチ回路68を介してExOR回路群66内の128個のExOR回路にそれぞれ送られると共に、Dラッチ回路68はイネーブル端子69の暗号化制御信号により128ビットの鍵情報かオールゼロかが切換制御される。

【0029】この図6の例において、ExOR回路群61は、C1エンコーダ52から遅延回路56、インバータ部57aを介して取り出される170バイトのデータとしての情報データ$C1_{170n+169}$～$C1_{170n+22}$及びパリティデータ$P1_{170n+21}$～$P1_{170n+14}$、$Q1_{170n+13}$～$Q1_{170n}$の内、先頭の20バイトのデータ$C1_{170n+169}$～$C1_{170n+150}$を除いた残り150バイトのデータ$C1_{170n+149}$～$Q1_{170n}$に対して排他的論理和（ExOR）回路を用いたデータ変換を行っているが、パリティデータについてはデータ変換を行わず、残り128バイトの情報データ$C1_{170n+149}$～$C1_{170n+22}$に対して、128ビットの鍵情報に応じたデータ変換を行わせるようにしてもよい。

【0030】この図6の回路においても、上記図2、図3の場合と同様な作用効果が得られることは勿論である。また、ExOR回路群61、66のいずれか一方のみを使用するようにしたり、いずれか一方あるいは双方の選択も暗号化の鍵として用いるようにすることもできる。

【0031】なお、上記データ変換手段としてのExOR回路群61、66の代わりに、AND、OR、NAND、NOR、インバート回路群等を使用してもよい。また、8ビット単位で1ビットの鍵情報あるいは鍵データによる論理演算を行う以外にも、8ビットの情報データに対して8ビットの鍵データで論理演算を行わせてもよく、さらに、情報データの1ワードに相当する8ビットの内の各ビットに対してそれぞれAND、OR、ExOR、NAND、NOR、インバート回路を組み合わせて使用してもよい。この場合には、例えば128バイトすなわち128×8ビットのデータに対して、128×8ビットの鍵データが用いられることになり、さらにAND、OR、ExOR、NAND、NOR、インバート回路を組み合わせて使用する場合には、これらの組み合わせ自体も鍵として用いることができる。また、論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。

【0032】また、上述した実施の形態においては、クロスインターリーブ型の誤り訂正符号の例について説明したが、図7に示すような積符号の場合にも同様に適用可能である。

【0033】この図7の例においては、20バイトのヘッダ部81と2052バイトのユーザデータ部82とから成るセクタ83の8セクタ分を、縦148バイト、横112バイトの2次元マトリクス構成とし、読み出し／書き込み方向であるR／W方向の148バイトに対してC1パリティ84を生成付加し、これに直交する方向の112バイトに対してC2パリティ85を生成付加している。これらのC1、C2パリティの交差する部分86は、C1符号化とC2符号化とが2重にかかっている。また、20バイトのヘッダ部81と同一行の図中斜線を付した部分87を除いたデータに対して、上記鍵情報に応じたデータ変換を施すようにする。

【0034】また、この積符号の場合にも、ヘッダ部81と同一列の部分88を除いたデータに対して、上記鍵情報に応じたデータ変換を施すようにしてもよく、さらに、ヘッダ部81と同一行の部分87及び同一列の部分88の両方を除いた部分に対してのみ、上記鍵情報に応じたデータ変換を施すようにしてもよい。

【0035】ここで、積符号の場合には、ヘッダ部81と同一行の図中斜線を付した部分87の全てを除かなくとも、ヘッダ部81のみを除くことができ、このヘッダ部81のみを除いた残りのデータに対して上記データ変換を行うようにしてもよい。なお、C1パリティのないものがLDC（ロングディスタンスコード）であり、これを誤り訂正符号に用いてもよい。

【0036】このように、誤り訂正符号化の際に取り扱われる中間データ等について、暗号化の鍵情報に応じた一部のデータに対してインバータ等でデータ変換を施すことにより、訂正不能誤りの発生確率が変化し、データ変換を施すデータ数に応じて暗号化のレベル、深度、解読の困難さ等が変化することになる。すなわち、用途に

応じて必要とされる暗号化の深度や難易度を、データ変換を施すデータ数により任意に設定でき、概要をサンプルとして提供したい場合や、正規ユーザ以外には再生不可能としたい場合や、セキュリティレベルの要求等に応じて種々の対応が図れる。

【００３７】また、セクタの先頭部分のヘッダ部については、上記データ変換が施されないため、セクタシンクやセクタアドレスの読み取りが迅速に行え、高速アクセスが可能である。

【００３８】ここで、上記誤り訂正符号化回路１６のみならず、上記図１のセクタ化回路１３、スクランブル処理回路１４、ヘッダ付加回路１５、変調回路１７、及び同期付加回路１８のいずれか少なくとも１つの回路は、入力に対して暗号化処理を施して出力するような構成を有することが挙げられる。このような暗号化処理の鍵情報は、記録媒体２１のデータ記録領域とは別の領域に書き込まれた識別情報、例えば媒体固有の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報、外部から供給される識別情報等を少なくとも一部に用いている。このように、媒体のデータ記録領域以外に書き込まれる識別情報は、例えば上記インターフェース回路１２からＴＯＣ（Table of contents ）生成回路２３を介して端子２４に送られる情報であり、また、インターフェース回路１２から直接的に端子２５に送られる情報である。これらの端子２４、２５からの識別情報が、暗号化の際の鍵情報の一部として用いられ、回路１３～１８の少なくとも１つ、好ましくは２以上で、この鍵情報を用いた入力データに対する暗号化処理が施される。

【００３９】この場合、回路１３～１８のどの回路において暗号化処理が施されたかも選択肢の１つとなっており、再生時に正常な再生信号を得るために必要な鍵と考えられる。すなわち、１つの回路で暗号化処理が施されていれば、６つの選択肢の１つを選ぶことが必要となり、２つの回路で暗号化処理が施されていれば、３０個の選択肢の１つを選ぶことが必要となる。６つの回路１３～１８の内の１～６つの回路で暗号化処理が施される可能性がある場合には、さらに選択肢が増大し、この組み合わせを試行錯誤的に見つけることは困難であり、充分に暗号の役割を果たすものである。

【００４０】また、暗号化の鍵情報を所定タイミング、例えばセクタ周期で切り換えることで、暗号化のレベルあるいは暗号の解き難さをさらに高めることができる。

【００４１】次に、図８は、記録媒体の一例としての光ディスク等のディスク状記録媒体１０１を示している。このディスク状記録媒体１０１は、中央にセンタ孔１０２を有しており、このディスク状記録媒体１０１の内周から外周に向かって、プログラム管理領域であるＴＯＣ（table of contents ）領域となるリードイン（leadin）領域１０３と、プログラムデータが記録されたプログラム領域１０４と、プログラム終了領域、いわゆるリードアウト（lead out）領域１０５とが形成されている。オーディオ信号やビデオ信号再生用光ディスクにおいては、上記プログラム領域１０４にオーディオやビデオデータが記録され、このオーディオやビデオデータの時間情報等が上記リードイン領域１０３で管理される。

【００４２】上記鍵情報の一部として、データ記録領域であるプログラム領域１０４以外の領域に書き込まれた識別情報等を用いることが挙げられる。具体的には、ＴＯＣ領域であるリードイン領域１０３や、リードアウト領域１０５に、識別情報、例えば媒体固有の製造番号等の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報を書き込むようにすると共に、これを鍵情報として、上述した６つの回路１３～１８の少なくとも１つ、好ましくは２つ以上で暗号化処理を施して得られた信号をデータ記録領域であるプログラム領域１０４に記録するようにする。再生時には、上記識別情報を、暗号を復号するための鍵情報として用いるようにすればよい。また、リードイン領域１０３よりも内側に、物理的あるいは化学的に識別情報を書き込むようにし、これを再生時に読み取って、暗号を復号するための鍵情報として用いるようにしてもよい。

【００４３】暗号化としては、上記誤り訂正符号化の際のデータ変換が必ず用いられており、上記ヘッダ部を除くデータに対してのみ暗号化の鍵情報に応じてデータ変換が施されることは勿論である。

【００４４】次に、本発明のデータ再生方法が適用されるデータ再生装置について、図９を参照しながら説明する。

【００４５】図９において、記録媒体の一例としてのディスク状記録媒体１０１は、スピンドルモータ１０８により回転駆動され、光学ピックアップ装置等の再生ヘッド装置１０９により媒体記録内容が読み取られる。

【００４６】再生ヘッド装置１０９により読み取られたディジタル信号は、ＴＯＣデコーダ１１１及びアンプ１１２に送られる。ＴＯＣデコーダ１１１からは、ディスク状記録媒体１０１の上記リードイン領域１０３にＴＯＣ情報の一部として記録された上記識別情報、例えば媒体固有の製造番号等の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報が読み取られ、この識別情報が暗号を復号化するための鍵情報の少なくとも一部として用いられる。この他、再生装置内部のＣＰＵ１２２から、再生装置固有の識別情報や、外部からの識別情報を出力するようにし、この識別情報を鍵情報の少なくとも一部として用いるようにしてもよい。なお、外部からの識別

情報としては、通信回線や伝送路等を介して受信された識別情報や、いわゆるＩＣカード、ＲＯＭカード、磁気カード、光カード等を読み取って得られた識別情報等が挙げられる。

【００４７】再生ヘッド装置１０９からアンプ１１２を介し、ＰＬＬ（位相ロックループ）回路１１３を介して取り出されたディジタル信号は、同期分離回路１１４に送られて、上記図１の同期付加回路１８で付加された同期信号の分離が行われる。同期分離回路１１４からのディジタル信号は、復調回路１１５に送られて、上記図１の変調回路１７の変調を復調する処理が行われる。具体的には、１６チャンネルビットを８ビットのデータに変換するような処理である。復調回路１１５からのディジタルデータは、誤り訂正復号化回路１１６に送られて、図１の誤り訂正符号化回路１６での符号化の逆処理としての復号化処理が施される。以下、セクタ分解回路１１７によりセクタに分解され、ヘッダ分離回路１１８により各セクタの先頭部分のヘッダが分離される。これらのセクタ分解回路１１７及びヘッダ分離回路１１８は、上記図１のセクタ化回路１３及びヘッダ付加回路１５に対応するものである。次に、デスクランブル処理回路１１９により、上記図１のスクランブル処理回路１４におけるスクランブル処理の逆処理としてのデスクランブル処理が施され、インターフェース回路１２０を介して出力端子１２１より再生データが取り出される。

【００４８】ここで、上述したように、記録時には、上記図１のセクタ化回路１３、スクランブル処理回路１４、ヘッダ付加回路１５、誤り訂正符号化回路１６、変調回路１７、及び同期付加回路１８の内の、誤り訂正符号化回路１６を含むいずれか少なくとも１つの回路において暗号化処理が施されており、この暗号化処理が施された回路に対応する再生側の回路１１４～１１９にて、暗号を復号化する処理が必要とされる。すなわち、上記図１のセクタ化回路１３にて暗号化処理が施されている場合には、セクタ分解回路１１７にて暗号化の際の鍵情報を用いた暗号の復号化処理が必要とされる。以下同様に、図１のスクランブル処理回路１４での暗号化処理に対応してデスクランブル処理回路１１９での暗号復号化処理が、図１のヘッダ付加回路１５での暗号化処理に対応してヘッダ分離回路１１８での暗号復号化処理が、それぞれ必要とされる。図１の誤り訂正符号化回路１６での暗号化処理は必ずなされており、これに対応して誤り訂正復号化回路１１６での暗号復号化処理が必要とされる。また、図１の変調回路１７で暗号化処理が施されている場合には、これに対応して復調回路１１５での暗号復号化処理が、さらに図１の同期付加回路１８での暗号化処理が施されている場合に対応しては同期分離回路１１４での暗号復号化処理が、それぞれ必要とされる。

【００４９】ここで、誤り訂正復号化回路１１６では、例えば上記図２、図３の誤り訂正符号化処理の逆処理が、図１０、図１１の構成により行われる。

【００５０】これらの図１０、図１１において、上記復調回路１１５にて復調されたデータの１７０バイトあるいは１７０シンボルを１まとまりとして、入力端子１４１に入力され、図１１のインバータ部１４２ａを有する再配列回路１４２を介し、遅延回路１４３を介して第１の復号器であるＣ１デコーダ１４４に送られている。このＣ１デコーダ１４４に供給される１７０バイトのデータの内２２バイトがＰ，Ｑパリティであり、Ｃ１デコーダ１４４では、これらのパリティデータを用いた誤り訂正復号化が施される。Ｃ１デコーダ１４４からは、１７０バイトのデータが出力されて、遅延回路１４５を介して第２の復号器であるＣ２デコーダ１４６に送られ、パリティデータを用いた誤り訂正復号化が施される。Ｃ２デコーダ１４６からの出力データは、図１０の遅延・Ｃ１デコード回路１４０に送られる。これは、上記遅延回路１４３及びＣ１デコーダ１４４と同様のものであり、これらの遅延回路１４３及びＣ１デコーダ１４４と同様の処理を繰り返し行うことにより誤り訂正復号化を行うものである。図１１の例では、遅延回路１４７及び第３の復号器であるＣ３デコーダ１４８で表している。この遅延回路１４７及びＣ３デコーダ１４８、あるいは遅延・Ｃ１デコード回路１４０で最終的な誤り訂正復号化が施され、パリティ無しの１４８バイトのデータが出力端子１４９を介して取り出される。この１４８バイトのデータは、上記図２、図３のＣ１エンコーダ５２に入力される１４８バイトのデータに相当するものである。

【００５１】そして、図２、図３の誤り訂正符号化回路の再配列回路５７のインバータ部５７ａで、インバータの有無による暗号化、すなわち、鍵情報に応じたデータ変換により、図１０、図１１の誤り訂正復号化回路の再配列回路１４２内のインバータ部１４２ａにて、対応する暗号復号化を行うことが必要とされる。ただし、上記データ変換は、ヘッダ部を除くデータに対してのみ施されているため、復号化もヘッダ部を除くデータに対してのみ行われる。この他、図２、図３と共に説明した各種暗号化処理に対応して、その暗号化を解くための逆処理となる暗号復号化が必要とされることは勿論である。

【００５２】次に、図１２は、上記図６の誤り訂正符号化回路の具体的構成に対応する誤り訂正復号化回路の具体的な構成を示す図である。

【００５３】この図１２において、上記図６の再配列回路５７の出力側に挿入されたExOR回路群６１に対応して、再配列回路１４２のインバータ部１４２ａの入力側及び遅延回路１４３の入力側の位置に、ExOR回路群１５１が挿入され、図６のＣ１エンコーダ５２の入力側に挿入されたExOR回路群６６に対応して、Ｃ３デコーダ１４８の出力側にExOR回路群１５６が挿入されている。

【００５４】これらのExOR回路群１５１、１５６は、上述したように、セクタのヘッダ部を除くデータに対する

データ変換を復号化するためのデータ変換を施すものであり、ExOR回路群１５１は、１５０個の８ビットExOR回路により、またExOR回路群１５６は、１２８個の８ビットExOR回路によりそれぞれ構成されている。なお、記録側の図６の誤り訂正符号化回路のExOR回路群６１で、パリティデータを除く１２８バイトの情報データに対して鍵情報に応じたデータ変換が施されている場合には、ExOR回路群１５１は１２８個の８ビットExOR回路により構成されることは勿論である。

【００５５】この図１２の端子１５２には、図６の端子６２に供給される鍵情報に相当する１５０ビットの鍵情報が供給され、いわゆるＤラッチ回路１５３を介してExOR回路群１５１内の１５０個の各ExOR回路にそれぞれ供給されている。Ｄラッチ回路１５３は、イネーブル端子１５４に供給された１ビットの暗号化制御信号に応じて、端子１５２からの１５０ビットの鍵情報をそのままExOR回路群１５１に送るか、オールゼロ、すなわち１５０ビットの全てを“０”とするかが切換制御される。また、ExOR回路群１５６については、１２８個のExOR回路を有し、鍵情報が図６の端子６７に供給される鍵情報と同様の１２８ビットであること以外は、上記ExOR回路群１５１の場合と同様であり、端子１５７に供給された１２８ビットの鍵情報がＤラッチ回路１５８を介してExOR回路群１５６内の１２８個のExOR回路にそれぞれ送られると共に、Ｄラッチ回路１５８はイネーブル端子１５９の暗号化制御信号により１２８ビットの鍵情報かオールゼロかが切換制御される。

【００５６】このように、誤り訂正回路のインバータを暗号化の鍵として使うことにより、簡易で大きな暗号化が実現できる。また、このインバータの数を制御することにより、絶対再生不可能な暗号化レベルのデータとか、エラー状態が悪くなると再生不可能となるデータとか、セキュリティレベルの要求に応じて対応できる。すなわち、インバータやExOR回路等の個数をコントロールすることにより、エラー状態の良いときは再生でき、悪くなると再生ができなくなるような制御も可能となり、また、エラー訂正のみでは回復不可能な絶対再生不可能状態を形成することもできる。また、暗号化の鍵としては、上記図示の例のように１箇所当たり百数十ビットもの大きなビット数となり、鍵のビット数の大きな暗号化ができるため、データセキュリティが向上する。しかも、このようなエラー訂正符号化回路やエラー訂正復号化回路を、いわゆるＬＳＩやＩＣチップのハードウェア内で実現することにより、一般ユーザからはアクセスが困難であり、この点でもデータセキュリティが高いものとなっている。

【００５７】また、セクタのヘッダ部のデータに対してはデータ変換が施されないため、再生時にヘッダ部内のセクタシンク（同期）やセクタアドレスについての暗号化の復号化のためのデータ変換が不要となり、高速アクセスが可能である。

【００５８】なお、本発明は、上記実施例のみに限定されるものではなく、例えば、データ変換としては、インバータやExORの例を示しているが、この他、ビット加算や、各種論理演算等によりデータ変換を行わせてもよいことは勿論である。この他、本発明の要旨を逸脱しない範囲で種々の変更が可能である。

【００５９】

【発明の効果】本発明によれば、誤り訂正符号化処理の際に取り扱われるデータの内のヘッダ部を除くデータに対して、暗号化の鍵情報に応じてデータ変換を施しているため、再生時にヘッダ部の暗号化を解く処理が不要となり、ヘッダ部のデータが迅速に得られるため、高速アクセスが可能である。また、誤り訂正処理である程度データ復元が可能な状態から、データ復元が行えない状態までの任意のレベルの暗号化が行える。これによって、エラー状態の良いときは再生でき、悪くなると再生ができなくなるような制御も可能となり、データ提供の用途に応じた、あるいはセキュリティレベルに応じた対応が可能となる。

【００６０】さらに、誤り訂正処理の中で鍵のビット数の大きな暗号化が可能であり、誤り訂正符号化や復号化ＩＣあるいはＬＳＩのような巨大なブラックボックスの中で暗号化を実現しているため、一般ユーザによる解読を困難化し、データセキュリティを大幅に向上させることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態が適用可能なデータ記録装置の概略構成を示すブロック図である。

【図２】誤り訂正符号化回路の一例の概略構成を示す図である。

【図３】誤り訂正符号化回路の一例の具体的な構成を示す図である。

【図４】セクタフォーマットの一例を示す図である。

【図５】クロスインターリーブ型誤り訂正符号の一例を示す図である。

【図６】誤り訂正符号化回路の他の具体例を示す図である。

【図７】積符号の場合の誤り訂正符号の一例を示す図である。

【図８】データ記録媒体の一例を示す図である。

【図９】本発明の実施の形態が適用可能なデータ再生装置の概略構成を示すブロック図である。

【図１０】誤り訂正復号化回路の一例の概略構成を示す図である。

【図１１】誤り訂正復号化回路の一例の具体的な構成を示す図である。

【図１２】誤り訂正復号化回路の他の例を示す図である。

【符号の説明】

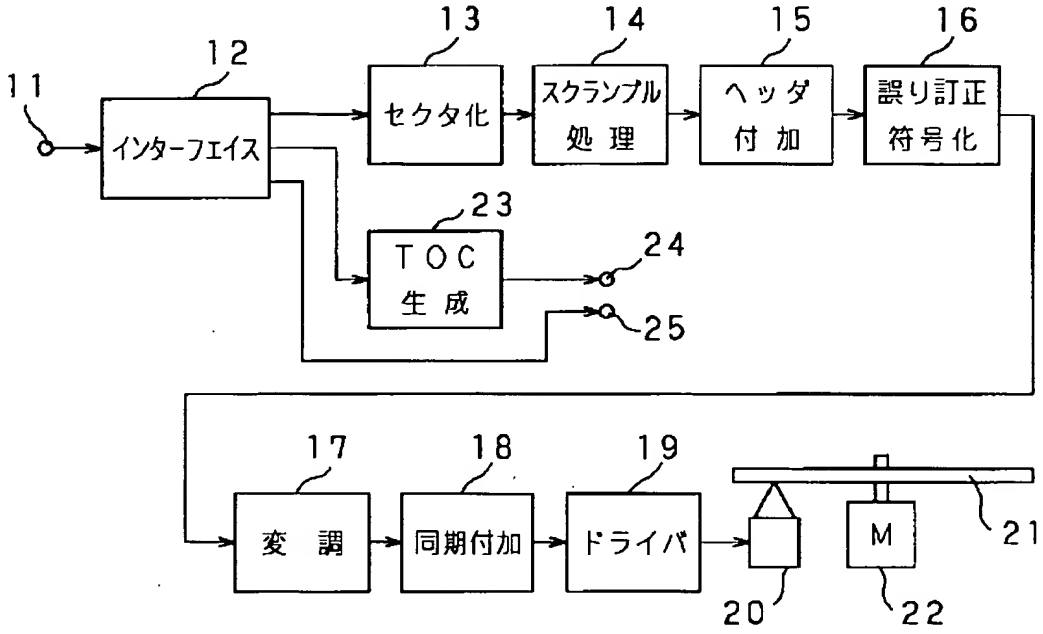
15

13　セクタ化回路
14　スクランブル処理回路
15　ヘッダ付加回路
16　誤り訂正符号化回路
17　変調回路
18　同期付加回路
52　C1エンコーダ
53、55、56、143、145、147　遅延回路
54　C2エンコーダ

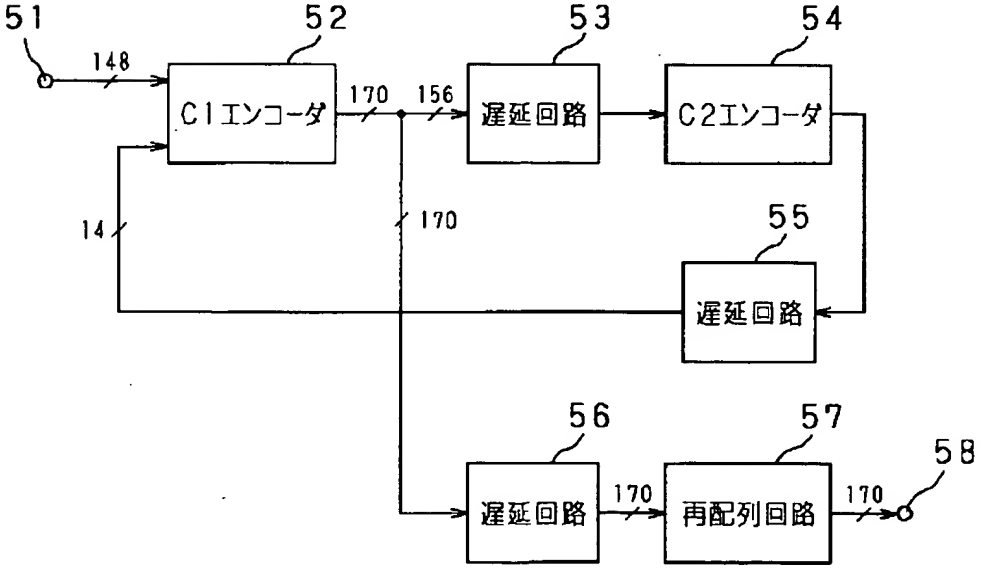
16

57、142　再配列回路
57a，142a　インバータ部
61、66、151、156　ExOR回路群
114　同期分離回路
115　復調回路
116　誤り訂正復号化回路
117　セクタ分解回路
118　ヘッダ分離回路
119　デスクランブル処理回路

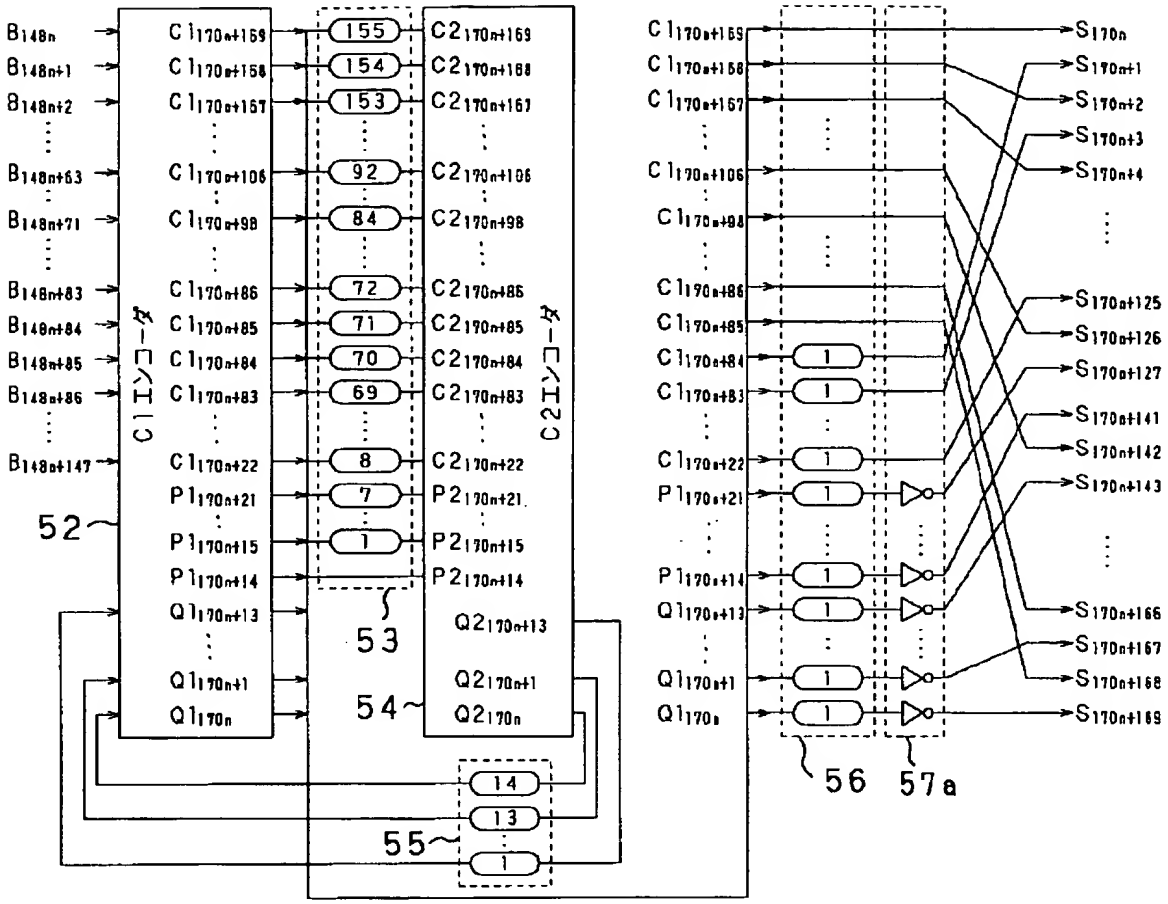
【図1】



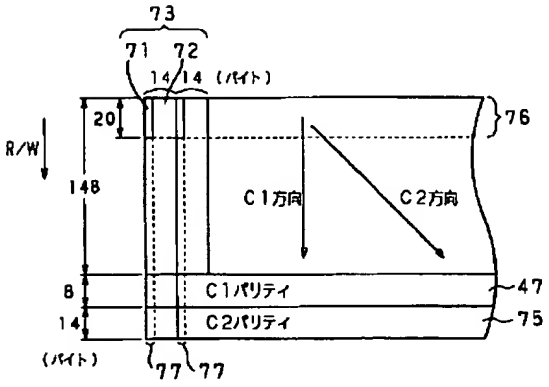
【図2】



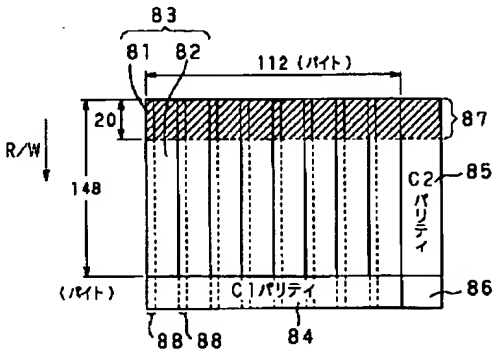
【図3】


C1エンコーダ
C2エンコーダ
52
53
54
55
56
57a

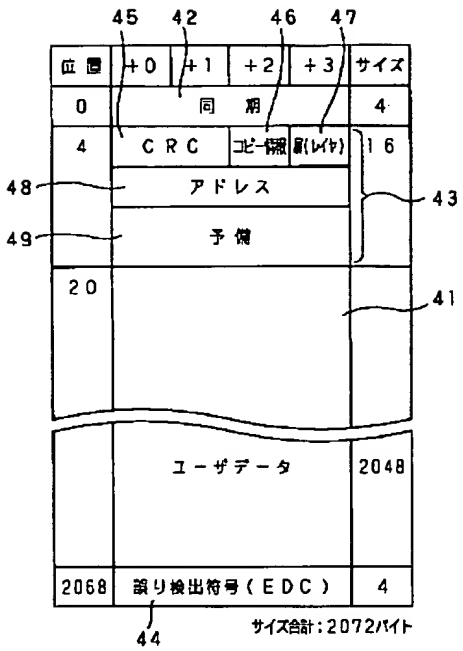
【図5】


73
71
72
14
14
(バイト)
20
76
R/W
148
C1方向
C2方向
8
C1パリティ
47
14
C2パリティ
75
(バイト)
77
77

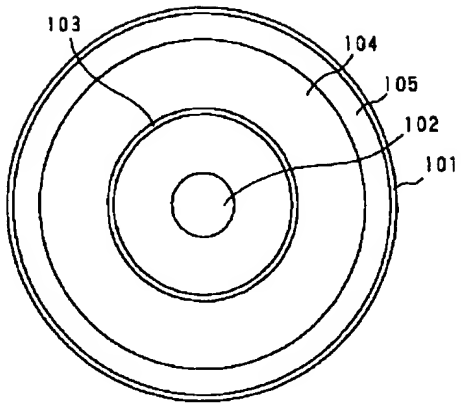
【図7】


83
81
82
112 (バイト)
20
87
R/W
148
C2パリティ
85
(バイト)
C1パリティ
86
88
88
84

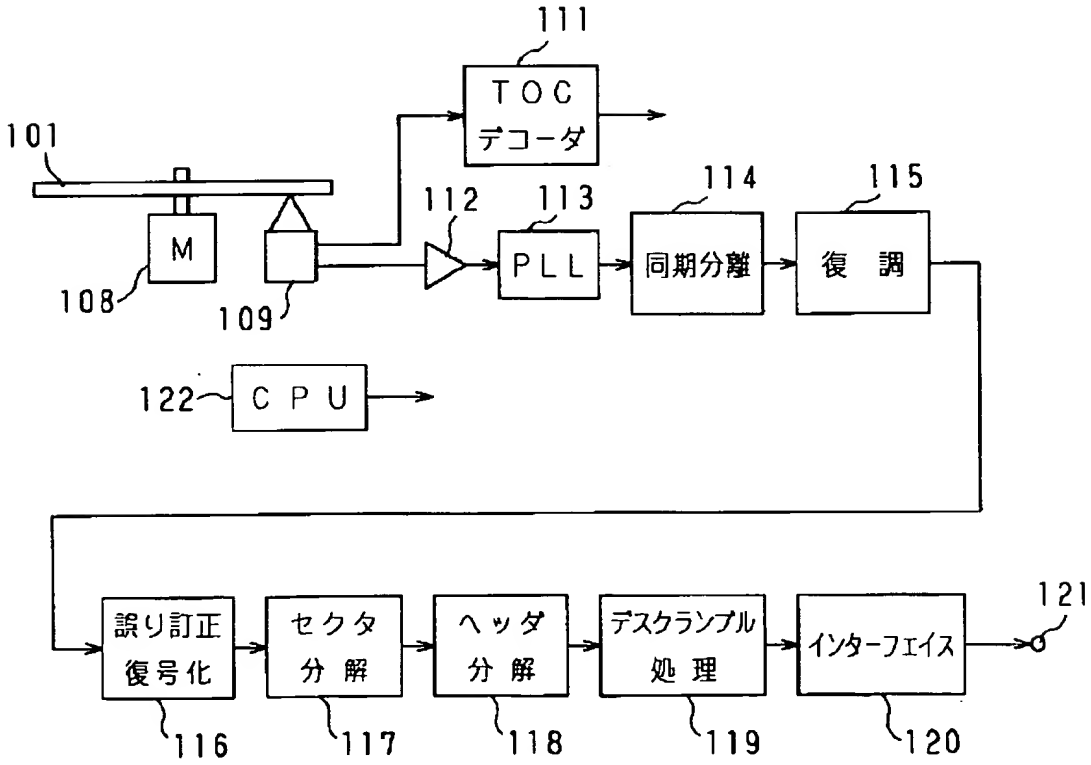
【図4】


45
42
46
47
位置
+0
+1
+2
+3
サイズ
0
同期
4
4
CRC
コピー情報
層(レイヤ)
16
48
アドレス
43
49
予備
20
41
ユーザデータ
2048
2068
誤り検出符号(EDC)
4
44
サイズ合計:2072バイト

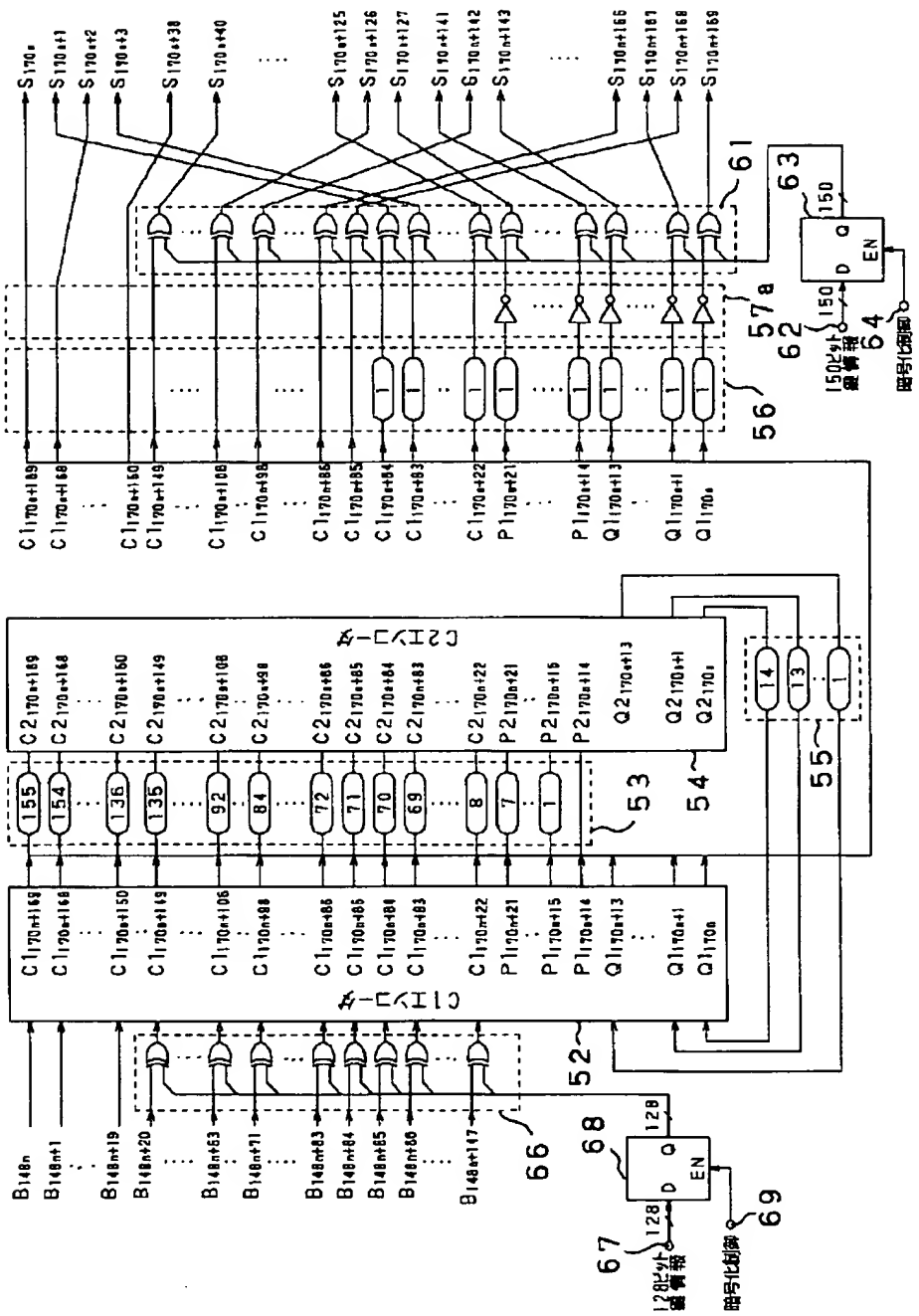
【図8】


103
104
105
102
101

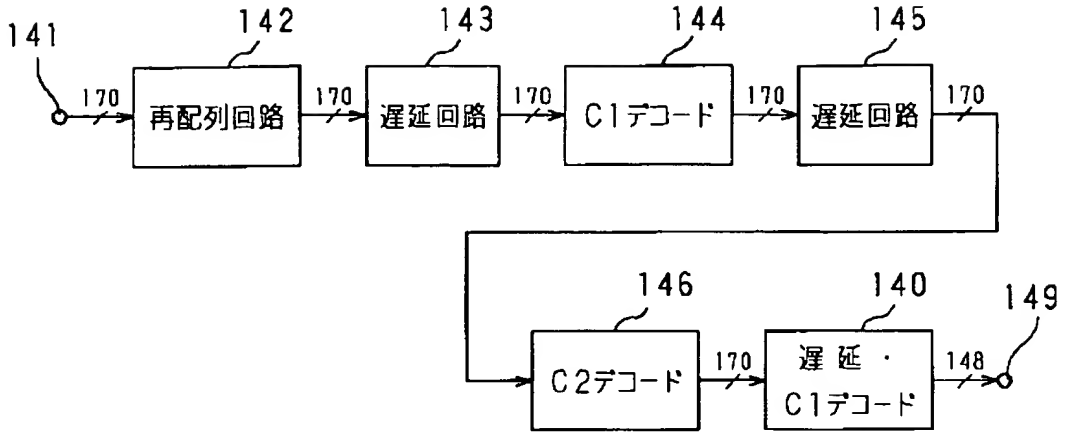
【図9】


111
TOC
デコーダ
101
112
113
114
115
M
PLL
同期分離
復 調
108
109
122
CPU
誤り訂正
復号化
セクタ
分 解
ヘッダ
分 解
デスクランブル
処 理
インターフェイス
121
116
117
118
119
120

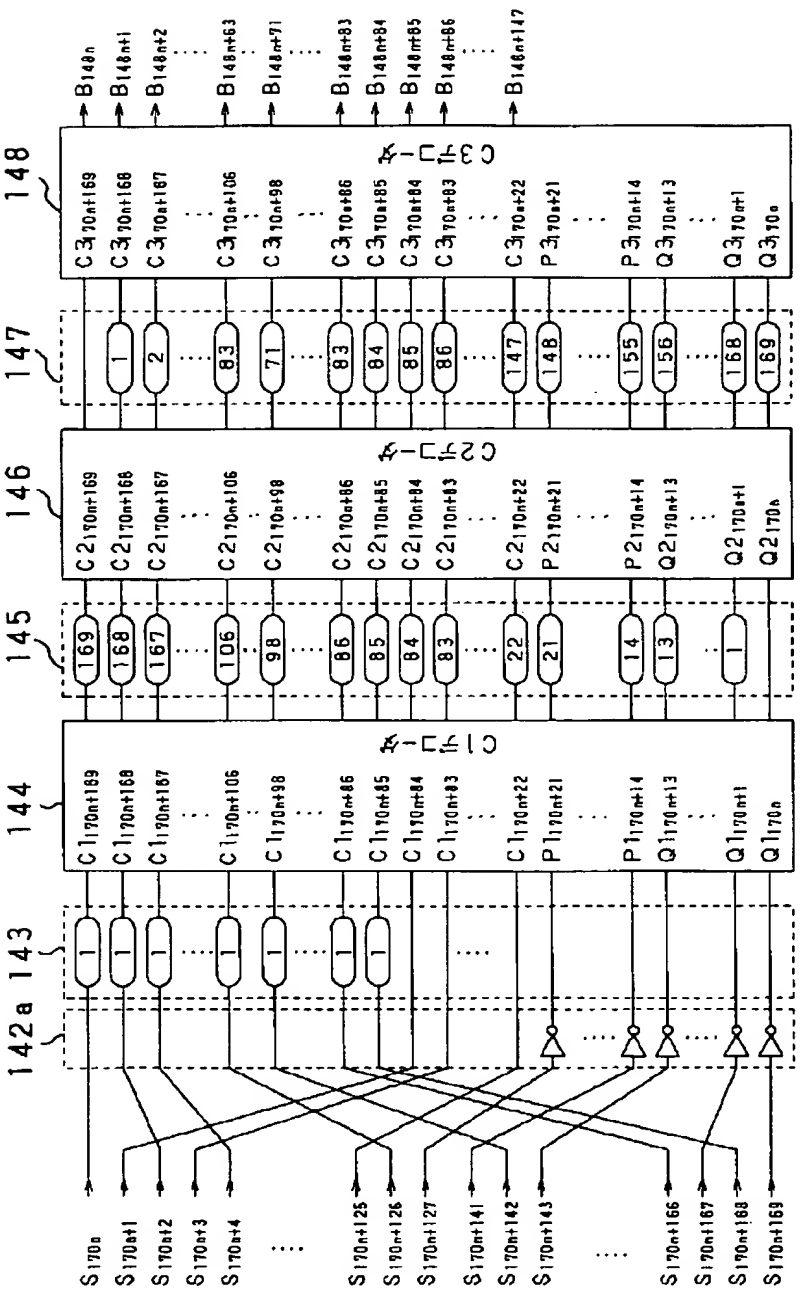
【図6】



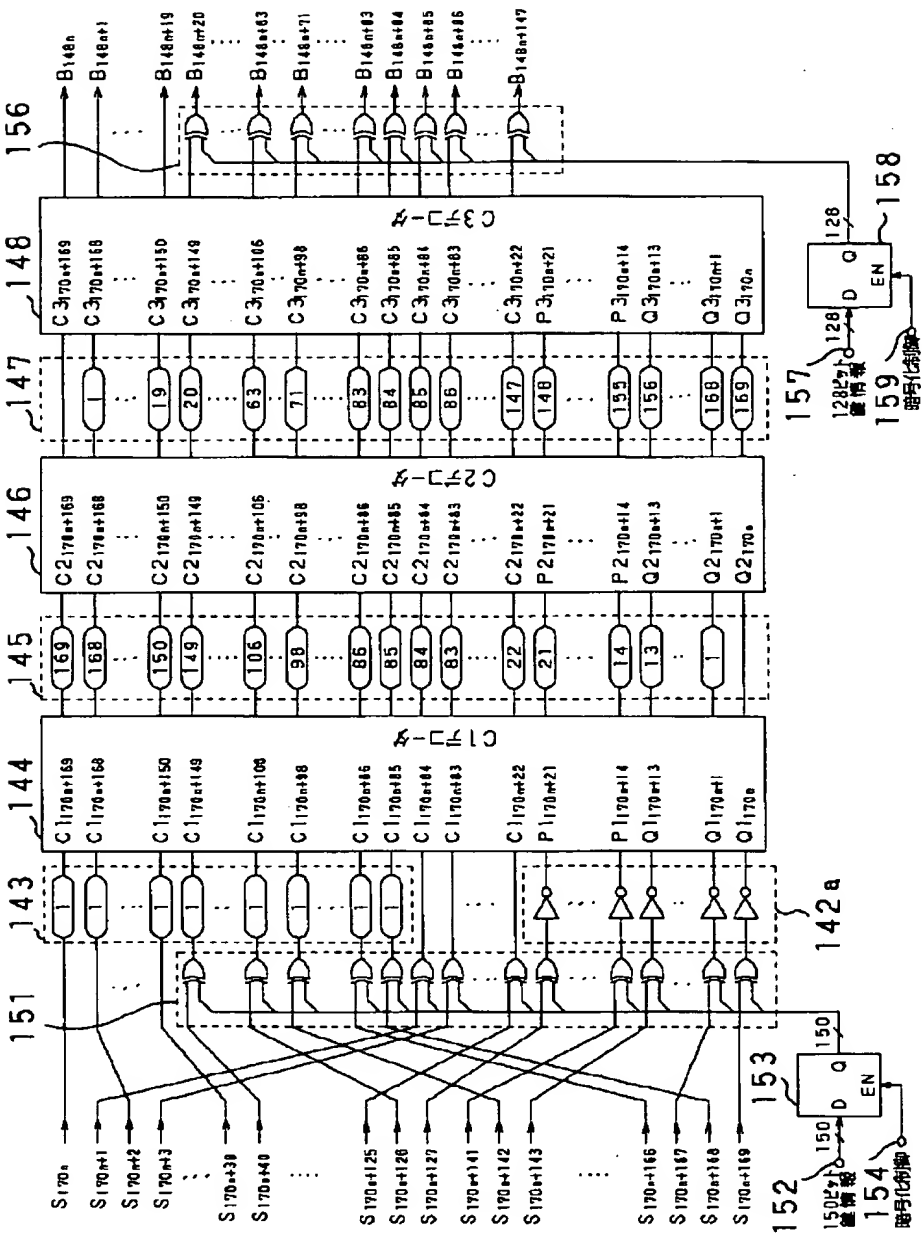
【図10】


141
142
143
144
145
170
再配列回路
遅延回路
C1デコード
遅延回路
146
140
149
C2デコード
遅延・
C1デコード
148

【図11】



【図12】



フロントページの続き

(51)Int.Cl.⁶	識別記号	庁内整理番号	FI		技術表示箇所
H04L 1/00			H04L 1/00	B	
9/18			9/00	651	

(72)発明者　川嶋　功
東京都品川区北品川6丁目7番35号　ソニー株式会社内